

## ⑫ 公開特許公報(A) 平4-155471

⑤ Int. Cl.<sup>3</sup>G 06 F 15/30  
15/21

識別記号

3 5 0  
3 4 0 C

庁内整理番号

6798-5L  
7218-5L  
8111-3E

⑬ 公開 平成4年(1992)5月28日

G 07 F 7/08

C※

審査請求 未請求 請求項の数 1 (全8頁)

⑭ 発明の名称 取引認証方式

⑯ 特 願 平2-279390

⑰ 出 願 平2(1990)10月19日

- ⑱ 発 明 者 岩 井 尚 史 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内  
 ⑱ 発 明 者 熊 井 康 子 東京都港区虎ノ門1丁目26番5号 エヌ・ティ・ティ・デ  
 ータ通信株式会社内  
 ⑱ 発 明 者 小 林 孝 文 東京都港区虎ノ門1丁目26番5号 エヌ・ティ・ティ・デ  
 ータ通信株式会社内  
 ⑲ 出 願 人 沖電気工業株式会社 東京都港区虎ノ門1丁目7番12号  
 ⑲ 出 願 人 エヌ・ティ・ティ・デ 東京都港区虎ノ門1丁目26番5号  
 ータ通信株式会社  
 ⑳ 代 理 人 弁理士 鈴木 敏 明  
 最終頁に続く

## 明 細 書

## 1. 発明の名称

取引認証方式

## 2. 特許請求の範囲

ICカードをICカードオフラインターミナルに挿入し、取引認証を行なう取引認証方式において、

上記ICカードは、個人識別用暗証番号データ、データ列を暗号化する第1のコード、データ列を暗号化する第2のコード、及びデータ列を暗号化する第3のコードが記録され、

上記ICカードオフラインターミナルは、前記第1のコード及び前記第2のコードと同一コードが記録され、

前記ICカードが作成した第1のデータ列を前記ICカード及びICカードオフラインターミナルの両方で前記第1のコードによりスクランブルし、該スクランブルした両方のデータの一致を検出する手段と、

前記ICカードオフラインターミナルが作成し

た第2のデータ列を、前記ICカードオフラインターミナル及びICカードの両方で前記第2のコードによりスクランブルし、該スクランブルした両方のデータの一致を検出する手段と、

前記オフラインターミナルに入力された暗証番号と、前記暗証番号データの一致を検出する手段と、

金融機関から送信された取引認証用のデータを前記オフラインターミナルに入力し、前記第3のコードによりスクランブルし、前記金融機関に送信する手段と、

前記金融機関にて受信した前記第3のコードによりスクランブルされた取引認証用データと、前記取引認証用のデータを該金融機関に記録された前記第3のコードと同一コードによりスクランブルされたデータとの一致を検出する手段とを有する取引認証方式。

## 3. 発明の詳細な説明

(産業上の利用分野)

本発明は、例えば銀行等の金融機関、あるいは

クレジット会社等によって発行されるキャッシュレスカードを用いて取引を行う場合に、確実に、取引認証をおこなう取引認証方式に関する。

(従来の技術)

近年は、キャッシュレス時代と呼ばれており、クレジット会社などに依り発行されたカードを使用することに依り、現金の取扱をせずに商品の購入が可能となっている。上記カードとしては、従来、プラスチックカード、エンボスカード、磁気ストライプカードなどが一般に使用されているが、これらのカードは構造上偽造が簡単であり、不正使用が問題となっている。このような問題を解決するため、最近ではカード内に、暗証番号等を記憶したIC回路を組み込み、暗証番号が外部から容易に読み出せないようにした情報カード、いわゆるICカードが開発されている。このICカードは、偽造が困難で、機密性に優れ、又、多数の情報を記憶できるという利点がある。しかし、上記のようなICカードを使用して実際に取引を行う場合には、銀行あるいは商店などに設置したIC

カードターミナルにICカードを装着し、暗証番号などを入力してカードおよびカード所有者の正当性を確認したのち所定の取引動作が行われるようにしている。

(発明が解決しようとする課題)

しかしながら、このようにICカードをターミナルに装着して暗証番号の照合を行う場合、第一に、例えば、商店などにおいて暗証番号の入力を行う際にその入力操作自体を視覚によって盗まれる可能性がある。又、第二に、例えば、ターミナル側に、カード所有者によって入力される暗証番号の情報を、暗証番号一致の信号を持って記憶する細工が施してある場合、真のカード所有者の暗証番号が上記ターミナルの設置される商店主等によって簡単に盗まれてしまう恐れもある。

そこで現在、カード所持者の暗証番号をカード発行時において予めカード内メモリに記憶させ、カード本体に設けたキーボードより入力される暗証番号と、上記メモリ内暗証番号とを比較照合し、その照合結果を即座にICカード自体に設けた表

示部にて表示するようにした、所謂、ターミナル側とはまったく接続関係を持たないで、独自に本人照合を行うことのできるICカードが考えられている。しかし、このような単独にて本人照合を行える機能を有するICカードであっても、そのカード自体が偽造される可能性がある。すなわちカード本体上の表示部にて、例えば、「本人OK」などの表示が行われたとしても、そのカード自体真に正当なカード会社から発行されたものかどうかを確認できないため、結局、真のカード所有者の認証を行うのは非常に困難なものとなる。

又、取引が成立した場合、金融会社と、商店との間で取引を確認する情報は、商品の購入金額、取引銀行口座番号、領収書の通し番号などを、特定の暗号コードでスクランブル化して得られるものであるが、上記情報は、通常、金融会社等と商店との文書での取引確認用に用いられるものであってその場での取引の確認にはなんら役にたっていない。

(課題を解決するための手段)

本発明は、上記のような問題点に鑑みなされたもので、カード所有者の暗証情報が不正に盗まれることなく、カード所持者と金融会社の相互の正当性を確実に認証する、取引認証システムを提供することを目的とする。

すなわちこの発明に係わる携帯型ICカードターミナルを用いた取引認証システムは、カード所有者特定用のデータをあらかじめ記憶させた個人証明カードを、携帯型ICカードターミナルに接続させ、カードとターミナルで相互認証を行いカードとターミナルの正当性を確認し、上記カード所有者にて入力される所有者特定用のデータと上記カード内カード所有者特定用データを比較照合し、本人の正当性を確認するとともに、商品の購入金額、クレジットの会員番号等を、金融会社等に送付し、それを基にして得られるデータを金融会社のホストコンピュータと携帯型ICカードターミナルの双方で、同一キー、同一アルゴリズムにてスクランブル化し、比較照合し、カード、ターミナルの正当性を金融会社のホストコンピュ-

タで確認し、取引の正当性を認証するように構成したものである。

#### (作用)

本発明は、ICカード及びICカードターミナルの双方に共通する第1及び第2のコードで、ICカードにて作成した第1のデータ列とICカードリーダで作成した第2のデータ列をスクランブル化するため、ICカードとICカードリーダそれぞれが正当であることを確認するとともに、暗証番号にて持主とICカードとの関係が正当であると確認できる。更に、金融機関から送信された取引認証用データを第3のコードでスクランブルするとともに、金融機関においても同一の第3のコードでスクランブルするので、ICカードターミナルと金融機関との関係も正当であると確認できる。従って、上記全ての確認を行うことによりICカード持主から金融機関に至る全ての関係が正当であると確認できるのである。

#### (実施例)

以下図面によりこの発明の一実施例を説明する。

面側に設けられた中央制御部22、相互／取引認証部25、音声出力装置(スピーカ)24、ICカード12との接続を図るための接続端子23を有する。一方表示部14は、液晶表示板26を有して構成されている。

次に、第1図に依り、上記ICカード12の回路構成について説明する。

ICカード12は、中央制御部31と、この中央制御部31に接続された、データメモリ32、PIN照合部34、相互認証部33、及びインターフェース部35と、インターフェース部35に接続された接続端子36とから構成される。データメモリ32には、ICカード12の発行時において、カード所有者本人が設定した暗証番号PIN、ICカード12とカードターミナル11の相互認証時に使用される暗号コード1、暗号コード2、取引認証番号生成に使用される暗号化コード3、および、本システムでの取引手順があらかじめ記憶されるとともに、例えば、商品取引に関する購入金額等のデータがその取引年月日とともに記憶

第2図はそのICカードオフラインターミナルを具体化した場合のカードターミナル11に点線を示すICカード12を装着した状態の概観構成図である。このカードターミナル11は、その本体上面にキーボード13および表示部14を有し、キーボード13の下側面にはICカード12との電氣的接続を図るためのカード挿入口15を有する。キー入力部13は、テンキー、ファンクションキー16などを備えている。ファンクションキー16には、暗証番号PIN(Personal Identification Number)や、取引認証番号SAN(Sales Approval No)を得るためのデータの入力終了を指示するENTERキー(ENT)や、カード内部に、取引手順が複数格納されている場合に、必要な取引を指定するためのカーソル移動キー(↑、↓)などがある。

次に、第3図は、上記カードターミナル11にICカード12を装着した状態でのA1-A2線縦断面構成を示すものである。カードターミナル11は、回路基板21と、この回路基板21の下

するために用いる記憶エリアが確保される。PIN照合部34は、カードターミナル11にて本人照合を行う際には、カード所有者にてキー入力される暗証番号PINと、上記データメモリ32にてあらかじめ記憶される真のカード所有者のPINとを比較照合するものである。この照合部34によりPIN一致と判定された場合には、上記カードターミナル11に対して本人OKのメッセージが送信される。相互認証部33は、カードターミナル11から送信される第1の乱数を、暗号コード1でスクランブルし上記カードターミナル11に対して送信するとともに、第2の乱数を生成し、上記カードターミナル11に対して送信する。カードターミナル11、この、第2の乱数を、暗号コード2でスクランブルし、ICカード12に送信する。暗号コード1でICカード12でスクランブルされた乱数と、上記カードターミナル11でスクランブルした乱数が一致すれば、上記カードターミナル11からは、上記ICカード12は、同一の暗号コード1をもつ、正当なICカードと

見なすことができる。一方、上記ICカード12が送信した第2の乱数を上記カードターミナルでスクランブルした乱数と、第2の乱数を上記ICカード12内で暗号コード2でスクランブルした乱数が上記ICカード12内で一致すれば、上記ICカード12からは、上記カードターミナル11は、同一の暗号コード2をもつ、正当なカードターミナルと見なすことができ、上記カードターミナル11に対して認証OKのメッセージが送信される。この様にして、カードターミナルに対するICカード及びICカードに対するカードターミナルの両方の相互認証処理を行なう。ここで、上記データメモリ32はEEPROMにて構成可能である。

次に第4図により上記カードターミナル11の回路構成について説明する。

カードターミナル11は中央制御部22と、この中央制御部22に接続された、キー入力部13を制御するキー入力制御部41、表示部14を制御する表示制御部42、及びスピーカ24を制御

取引認証番号生成部45は、後述する様に、相互認証、PIN照合後、本取引を行なう際に用いるもので、キー入力部13から入力された取引認証番号生成番号と、ICカード12のデータメモリ32より読み出した暗号化コード3を用いてスクランブルすることにより取引認証番号を生成するものである。この取引認証番号は、インターフェース部49を介して、中央制御部22に送信される。

次に、上記のように構成されるICカードオフラインターミナルを用い、ICカード12による商品取引の際に、その場でカード取引認証番号を算出表示する動作を5図に示すフローチャートを用いて説明する。

まず、カード所有者は、商品の購入を行うに際して、商品との間で取引が成立すると、上記カードターミナル11のカード挿入口15に対してICカード12を挿入する。すると、ICカード12は、第3図で示したように、カードターミナル11のカード装着部に装着され、カード側の接続端子

する音声出力制御部50を有する。更に、中央制御部22には、演算部43と、インターフェース部49を介してICカード用接続端子23と相互／取引認証部44が接続される。上記相互／取引認証部44は、上記インターフェース部49介して中央制御部22からのコマンドを実行するもので、取引認証番号生成部45、相互認証部46、制御演算部47、データメモリ48が備えられている。メモリ48には、相互認証処理用の暗号コード1及び暗号コード2が記憶されている。相互認証処理の場合、上記インターフェース部49を介して上記相互／取引認証部44に相互認証コマンドが送信されると、上記相互／取引認証部44の上記相互認証部46のプログラムが起動され、上記メモリ48の暗号コード1及び2を用いて、インターフェース部49を介してICカード12との間で前述した相互認証処理を行い、お互いに正当であると認められた場合には、上記インターフェース部49を介して上記中央制御部22に相互認証OKのメッセージを送信する。

36とICカード用接続端子23が接続状態となる。ここで、中央制御部22は、ステップS1において、相互認証コマンドをインターフェース部49を介して相互／取引認証部44に送信する。相互／取引認証部44は、相互認証プログラム46を起動し、相互認証プログラム46に従って第1の乱数を生成する。生成された第1の乱数は、インターフェース部49およびICカード用接続端子23を介してICカード内の相互認証部33に送られる。又、インターフェース部49を介してメモリ48に記憶されている相互認証用暗号コード1を用いてスクランブル化され、メモリ48に記憶される。一方、インターフェース部49およびICカード用接続端子23を介して送られた第1の乱数を受信したICカード内の相互認証部33は、第1の乱数をデータメモリ32に記憶されている相互認証用暗号コード1を用いてスクランブル化するとともに第1のスクランブル(乱数)、第2の乱数を生成し、データメモリ32に記憶されている相互認証用暗号コード2を用いてスクラ

ンブル化しデータメモリ32に記憶する(第2のスクランブル乱数)。さらに、データメモリ32に記憶されている相互認証用暗号コード1を用いてスクランブル化された乱数と第2の乱数とをICカード用接続端子23およびインターフェース部49を介して相互/取引認証部44に送る。第1のスクランブル乱数と第2の乱数を受信した、相互/取引認証部44は、第1のスクランブル乱数とメモリ48に記憶された相互認証用暗号コード1を用いてスクランブル化された乱数1とを比較し、一致した場合には、ICカード12は、カードターミナル11と同一の相互認証用暗号コード1を持っていると判断し、相互/取引認証部44は、ICカード12を正当なカードとみなして処理を続ける。一致しなかった場合には、ICカード12は、カードターミナル11と同一の相互認証用暗号コード1を持っていないと判断し、相互/取引認証部44は、ICカード12を不正なカードとみなしてインターフェース部49を介して中央制御部22にカードNGのメッセージを送信

に送る。一致しなかった場合には、カードターミナル11は、ICカード12と同一の相互認証用暗号コード2を持っていないと判断し、ICカード内の相互認証部33は、カードターミナル11を不正なターミナルとみなして認証NGのメッセージを、ICカード用接続端子23およびインターフェース部49を介して相互/取引認証部44に送る。ステップS2において、中央制御部22は、認証NGのメッセージを受信した場合には、表示制御部42を介してLCD14にエラーを表示し、処理を停止する。認証OKのメッセージを中央制御部22が受信した場合には、中央制御部22は、ステップS3において、インターフェース部49およびICカード用接続端子23を介してICカード12のデータメモリ32に記憶されている本システムでの取引手順をよみだし、以下、その手順に従って動作する。本実施例では、暗証入力がOKとなった後に、取引認証番号を生成するものとする。

暗証番号の入力が必要な場合、中央制御部22

し、処理を終了する。第1のスクランブル乱数とデータメモリ48に記憶された、メモリ48に記憶されている相互認証用暗号コード1を用いてスクランブル化された乱数1とを比較し、一致した場合には、相互/取引認証部44は、受信した、乱数2をメモリ48に記憶されている相互認証用暗号コード2を用いてスクランブル化し、インターフェース部49およびICカード用接続端子23を介してICカード内の相互認証部33に送る。インターフェース部49およびICカード用接続端子23を介して送られた乱数2を受信した、ICカード内の相互認証部33は、第2の乱数と、データメモリ32に記憶されている第2のスクランブル乱数と比較し、一致した場合には、カードターミナル11は、ICカード12と同一の相互認証用暗号コード2を持っていると判断し、ICカード内の相互認証部33は、カードターミナル11を正当なターミナルとみなして認証OKのメッセージを、ICカード用接続端子23およびインターフェース部49を介して相互/取引認証部44

は、表示制御部42を介してLCD14に、カード所有者に、暗証入力を促すメッセージを表示する。カード所有者は、ステップS4において、カードターミナル11のキー入力部13より暗証番号PINをキー入力する。すると、このキー入力によるPINデータは、キー入力制御部41を介して中央制御部22に入力された後インターフェース部49およびICカード用接続端子23を介してICカード内のPIN照合部34に送られる。そして、このPIN照合部34にてラッチされたキー入力によるPINデータは、ステップS5において、データメモリ32にてあらかじめ記憶される本カード12の真の所有者の暗証番号PINと比較照合されるので、ここで、キー入力によるPINと真のPINとが一致し、上記ステップS1におけるPINのキー入力者は、本カード12の真の所有者であると判定されるとステップS6に進み中央制御部31は、カードターミナル11に対して、本人OKのメッセージを送信する。これにより、カードターミナル11の表示部14には、

表示制御部42を介して本人OKのメッセージが表示されるようになり、このOKメッセージが表示されたままの状態、カードターミナル11を商店オペレータに渡すことにより、オペレータはカード所持者の正当性を確認することができる。

一方、上記ステップS6にて、カードターミナル11に対して、本人OKのメッセージが入力されない場合には、上記表示部14には、エラーメッセージが表示され、商店オペレータは、上記PIN入力者が不正なカード所持者であることを確認することができる。

こうして、カード所有者の正当性が確認されると、商店オペレータは、カードターミナル11の表示部14の表示に従い、いずれかのキーを押下する。すると、カードターミナル11は、取引認証番号生成のためのキー入力待ち状態となる。ここで、商店オペレータは、電話あるいはオンラインアクセスでクレジット会社にクレジット会員番号などの、カード所持者を特定できる情報と、購入金額などの取引を特定できる情報を伝える。ク

ドにより、ステップS10において取引認証番号生成プログラムを起動し、暗号化コード3にて取引認証番号生成番号をスクランブル化する。このスクランブル化されたデータを、取引認証番号とし、ステップS11においてインターフェース部49を介して中央制御部22に入力され、表示制御部42を介して表示部14にて表示出力されるようになる。ここで、商店オペレータは、表示出力された取引認証番号を、クレジット会社に伝える。クレジット会社では、暗号化コード3と同一のコードを用いて、取引認証番号生成番号をスクランブル化し、商店オペレータより伝えられた、取引認証番号と比較する。クレジット会社でスクランブル化した取引認証番号生成番号と、カードターミナル11でスクランブル化した取引認証番号生成番号が一致すれば、クレジット会社は、正当なカード12を、正当なカードターミナル11で、正当な所有者が、使用した、正当な取引である、と判断し、商店オペレータに、取り引きの成立を伝える。クレジット会社でスクランブル化し

クレジット会社では、クレジット会員番号から、クレジット会社で管理している、ICカード12のデータメモリ32に記憶されている取引認証番号生成に使用される暗号化コード3と同一のコードを検索し、本コードと、購入金額などの取引を特定できる情報から、取引認証番号生成番号を作り出し、商店オペレータに伝える。商店オペレータは、ステップS7において、カードターミナル11のキー入力部13よりクレジット会社から伝えられた、取引認証番号生成番号を入力する。このキー入力による取引認証番号生成番号は、キー入力制御部41を介して中央制御部22に入力された後インターフェース部49を介して相互／取引認証部44に、ステップS8においてICカード用接続端子23およびインターフェース部49を介して読み出されたICカード12のデータメモリ32に記憶されている取引認証番号生成に使用される暗号化コード3とともにステップS9において取引認証番号生成コマンドとして送られる。相互／取引認証部44は、取引認証番号生成コマン

ドした取引認証番号生成番号と、カードターミナル11でスクランブル化した取引認証番号生成番号が一致しなければ、カード12、または、カードターミナル11、若しくは、その双方が、不正なものである、と判断し、商店オペレータに、取り引きの不成立を伝える。

取引が成立した場合、このカード取引認証番号は、各商店ごとに設置されているエンボスインプリントにより領収書に印字され、カード所有者に渡される。ここで、カード所有者が上記オペレータより渡された領収書にサインをし、ICカードによる取り引きの全過程を終了する。

したがってこのように構成されるオフラインターミナルを用いれば、安全で、確実な、カード取引が、容易に、実現可能となる。

尚、上記実施例においては、取引認証番号をLCD14にて表示し、それを、商店オペレータが、クレジット会社に伝えているが、このデータは、例えば、スピーカ24を介して、DTMF音

として出力してもよい。又、カード所持者の正当性を、PINで証明しているが、本オフラインターミナルに、イメージリーダをもうけ、指紋などのイメージ情報にてカード所持者の正当性を証明するようにすれば、システムの安全性は、より高まる。又、記実施例においては、商店での取り引きを例に上げたが、本オフラインターミナルを個人で所有していれば、電話等での通信販売等において利用しても確実に本人確認が可能であるので、サービス提供者、カード所持者、の双方に安全なシステムを提供することが可能となる。

#### (発明の効果)

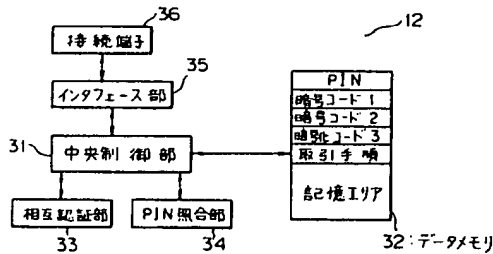
以上のようにこの発明によれば、予めカード所有者特定用のデータが記憶されるICカードとの電氣的接続を図るカード装着部と、売買金額などの取り引きデータを入力するキー入力部をもうけ、カードとカードターミナルの相互認証を行い、上記カード装着部にて接続状態にあるICカードより読み取ったカード所有者特定用のデータと上記キー入力部より入力される取引データに基づきカ

ード取引認証番号を算出し、これを、クレジット会社等で算出した結果と比較するように、構成したので、カードの不正、ターミナルの不正、所持者の不正等を、容易に発見することが可能となり、きわめて安全なカード取引方式を構築することが可能となる。

#### 4. 図面の簡単な説明

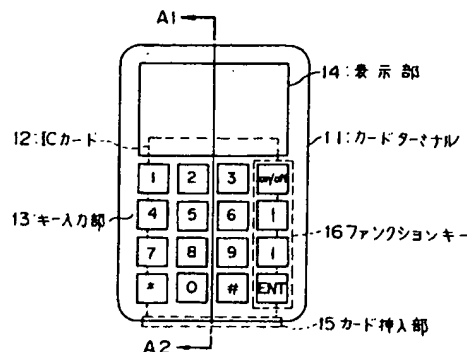
第1図は本発明の取引認証方式に用いるICカードの回路図、第2図は本発明の取引認証方式に用いるICカードオフラインターミナルの概観図、第3図は第2図におけるA1-A2線断面図、第4図は本発明の取引認証方式に用いるICカードカードターミナルの回路図、第5図は本発明の取引認証方式における一実施例のフローチャート。

11…ICカードターミナル、12…ICカード、22…中央制御部、33…相互認証部、34…PIN照合部、32…データメモリ。



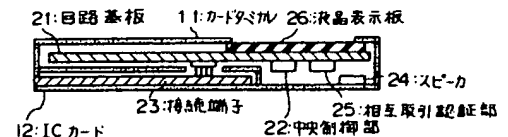
本発明の取引認証方式に用いるICカードの回路図

第1図



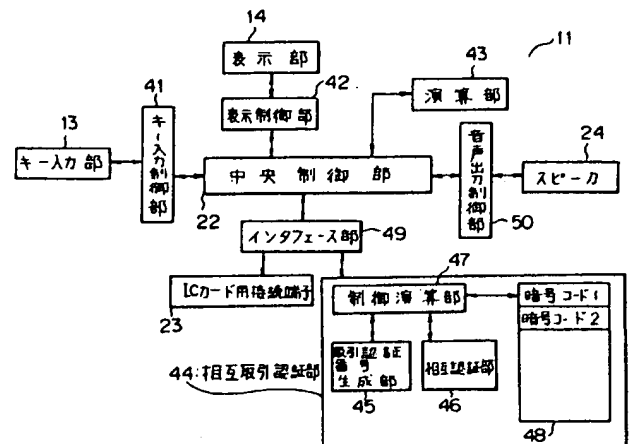
本発明に用いるICカードオフラインターミナル

第2図



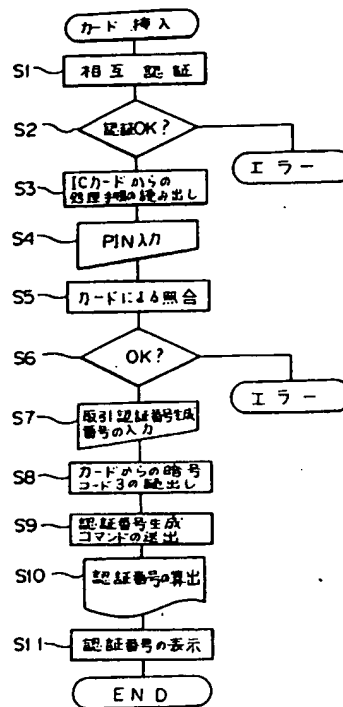
第2図のICカードターミナルのA1-A2線断面図

第3図



本発明の取引認証方式に用いるICカードターミナルの回路図

第4図



取引認証方式の動作フローチャート

第 5 図

第 1 頁の続き

⑤Int. Cl. 5

G 06 F 15/30

G 06 K 17/00

G 07 F 7/12

識別記号	庁内整理番号
3 4 0	C 6798-5L
	6798-5L
	S 6711-5L